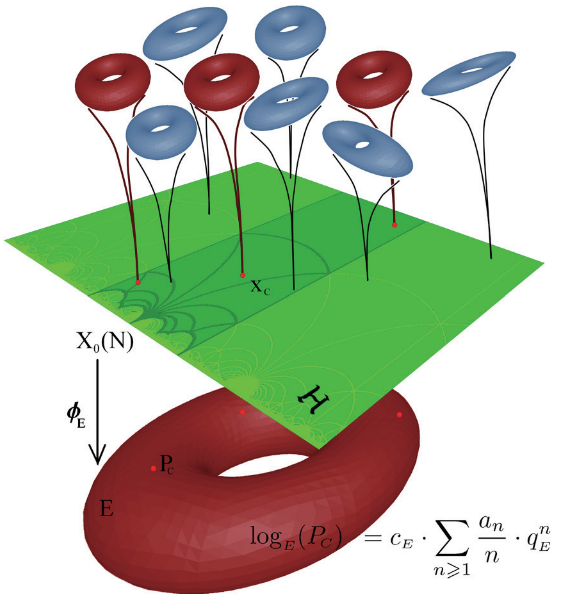
浅说椭圆曲线

陆 俊



一、费马先生的金蛋：椭圆曲线

在所有律师里面数学最好的是谁？毫无疑问是法国的费马（Pierre de Fermat）—— 一位充满传奇色彩的业余数学家。 他在数学领域做了许多重要的开创性工作，足以媲美任何同时代的数学家。至今，我们还常常能在数学课本中见到他的名字。

比如说到解析几何，很多人只知道笛卡尔的大名，殊不知费马也是解析几何的创始人。他早就用坐标方法（即方程）去研究几何图形的性质。费马首先指出一次方程。

$$ax+by+c = 0.$$

可以表示直线。接着，他注意到二次方程可以表示圆锥曲线（即椭圆、双曲线和抛物线），并且知道如何用坐标变换研究它们的一般形式，这正是中学时代经常折磨我们的玩意儿。

费马（1601-1665）

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1 \quad（椭圆）$$

$$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1 \quad（双曲线）$$

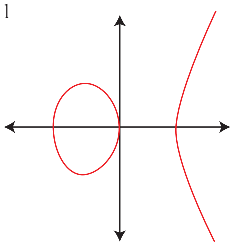
$$y^2=ax \quad（抛物线）$$

如果你是费马，有了这些发现之后，很自然会去思考三次方程定义的曲线，对不对？费马当然也会这么想。首先，在一个合适的坐标变换后，大多数三次方程可以写成标准形式

$$y^2 = x^3+ax+b,$$

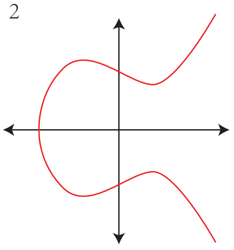
其中系数 a, b 满足 $4a^3+27b^2 \neq 0$，这个方程描绘出来的曲线就叫做**椭圆曲线**。后面我们再介绍不满足这个条件的曲线。下面的两张图都是椭圆曲线

1



$y^2=x^3-x$

2

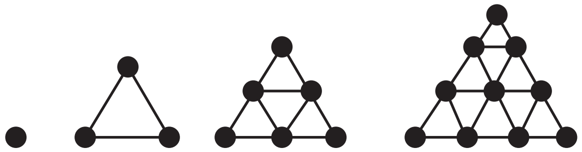


$y^2=x^3-x+1$

费马的许多研究都围绕着椭圆曲线。让我们循着费马的轨迹，一起来欣赏一下这些有趣的工作（有兴趣的读者可以参看加藤和也等人写的《数论 I: Fermat 的梦想和类域论》）。

(A) 立方数与三角数

所谓三角数，就是下面这类等边三角形上的格点个数：1，3，6，10，15，……。



你很容易猜出三角数的一般公式是 $n(n+1)/2$.

费马叙述了以下几个有趣的结果：

(1) 除了 1 之外，任何三角数都不可能是立方数。用方程的语言，就是说

$$\frac{y(y+1)}{2}=x^3$$

除了 $(x, y) = (1,1)$ 之外没有其他正整数解。上面这个方程描绘的曲线是椭圆曲线——当然你需要做一些坐标变换才能变成标准型。

(2) 一个立方数减去 2 不可能是平方数 , 除非是以下特例：$5^2 = 3^3 - 2$. 写成方程的话，就是

$$y^2 = x^3 - 2$$

仅有一组正整数解 $(x, y) = (3, 5)$。这方程描绘的曲线当然还是椭圆曲线。

(3) 一个立方数减去 4 不可能是平方数 , 除非是以下特例：$2^2 = 2^3 - 4$, $11^2 = 5^3 - 4$。也就是说方程

$$y^2 = x^3 - 4$$

仅有两个整数解 $(x, y) = (2, 2)$ 和 $(5, 11)$。上面的方程仍然描绘了椭圆曲线。

(B) 直角三角形与同余数

所谓的同余数，来自于以下经典的数学问题。

> **（同余数问题）**给定正整数 n, 是否存在直角三角形，使得三条边都是有理数，并且面积恰好是 n? 如果存在这样的三角形，就称 n 是同余数。

费马在丢番图《数论》的空白处做的批注中叙述了这样的结果：

$n = 1, 2$ 不可能是同余数。

同余数问题由来已久，至今仍未彻底解决。 目前我们已知的最前面的同余数是

5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39,41, 45, 46,47

同余数问题等价于求解正有理数 (a, b, c) 满足：

$$a^2+b^2=c^2,\quad n=\frac{ab}{2}.$$

如果我们令

$$x=\frac{n(a+c)}{b},\quad y=\frac{2n^2(a+b)}{b^2},$$

则得

$$y^2 = x^3 - n^2x.$$

这个方程再一次向我们呈现了椭圆曲线！显然 $(x, y) = (0, 0)$, $(n, 0)$，$(-n, 0)$ 是它的有理数解。正整数 n 是否是同余数 , 取决于上面的方程还有没有其他有理数解。

费马的另一个结论说：

> 假如 n 是同余数 , 那么上面的椭圆曲线方程应该还有无限多个有理数解。

例如，因为 5 是同余数，所以椭圆曲线方程 $y^2=x^3-25x$ 就有无限多个有理数解。

一般说来，判断一条椭圆曲线的方程是否有无限多个有理数解，是一个困难的问题。这个问题涉及到数学上最著名的猜想之一 —— BSD 猜想。这个重要的猜想曾作为千禧年七大数学猜想为世人所知，吸引了许多数学家为之奋斗。它将数学中很多深刻的理论分支都联系在一起。如果能解决它，那么数学的发展必将会飞跃一大步。

(C) 费马大定理

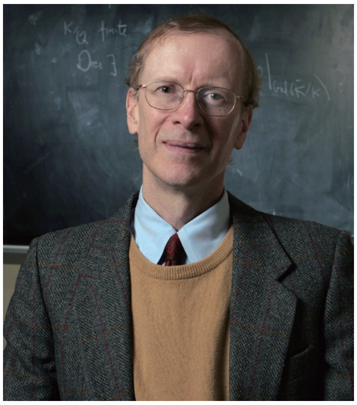
费马曾经在丢番图的书的批注中提出如下的“结论”（称为费马猜想、费马的最后定理、费马大定理）：

以下方程

$$X^n + Y^n = Z^n \ (n>2),\quad XYZ \neq 0$$

没有整数解 (X, Y, Z).

费马自己证明了 $n = 4$ 的情形 , 并声称找到了一种巧妙的方法能够解决一般情形。但是他并没有告诉人们一般情形



怀尔斯（1953- ）

证明是怎样的。此后的几百年，有许许多多优秀的数学家致力于证明这个结论，但他们的努力都失败了。直到 1995 年前后，才由数学家怀尔斯（Andrew Wiles）彻底解决。

虽然许多人证明费马猜想的努力都未获成功，但是他们的工作却在很大程度上促进了各个数学分支的发展，极大地丰富了数学世界的内容。因此有人把费马猜想比喻作“一只会生金蛋的鸡”，实在是非常地准确。

如今回过头来看，我们不得不问：对于如此之难的数学问题，为何费马会声称自己找到了证明？到底是费马跟我们开了玩笑，还是上帝跟费马开了玩笑？这里不做探讨了。我们想要告诉大家的是，费马猜想和椭圆曲线的关系是极为密切的。从某个方面说，椭圆曲线是不折不扣的“金蛋”！

让我们来看几个具体的例子。

例 1：$X^3 + Y^3 = Z^3$.

这个特殊情形由高斯和欧拉分别解决。欧拉的证明极为繁琐，相比之下高斯的方法不但简洁，而且极富启发性。我们这里不打算介绍证明，有兴趣的读者可以参看 H. 德里《100 个著名初等数学问题》一书。

让我们做这样的初等变换：

$$x = \frac{12Z}{X+Y}, \quad y = \frac{36(X-Y)}{X+Y}.$$

将上式代入费马方程即得

$$y^3 = x^3 - 432.$$

瞧，这又是椭圆曲线！因为我们现在已经知道原来的方程没有非平凡解(所谓平凡解，就是允许 X, Y, Z 其中一个数是零)，所以这相当于说上面的椭圆曲线方程只有显然的有理数解 (12,36) 和 (12,-36).

例 2：$X^4 + Y^4 = Z^4$.

费马利用无穷递降法证明其无平凡解。它也可以通过以下初等变换变成椭圆曲线：

$$x = \frac{2(Y^2+Z^2)}{X^2}, \quad y = \frac{4Y(Y^2+Z^2)}{X^3}.$$

代入原方程即得一条椭圆曲线

$$y^2 = x^3 - 4x.$$

它仅有 (0,0), (2,0) 和 (-2,0) 三个有理数解。我们也可以用另一种方法得到椭圆曲线。令 $x = Z^2 / Y^2$, $y = X^2Z / Y^3$, 这就得到新的椭圆曲线

$$y^2 = x^3 - x.$$

例 3：$X^n + Y^n = Z^n$, n 是素数（所谓素数，就是指不能分解成两个更小的正整数的乘积的正整数）。

假设 $(X, Y, Z) = (a, b, c)$ 是一组非平凡解。此时人们构造了椭圆曲线 (它不是标准方程)

$$y^2 = x(x+a^n)(x - b^n).$$

这条椭圆曲线称作弗雷曲线（Frey Curve）。里贝特（Kenneth Alan Ribet）于 1986 年证明该曲线不能是模曲线（这里我们不解释此概念）。而另一方面怀尔斯于 1995 年证明谷山 - 志村猜想（Taniyama–Shimura conjecture），即任何椭圆曲线都是模曲线，这就等于证明费马方程无非平凡解。

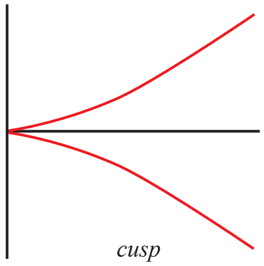
如果 n 是大于 4 的合数，上面的几类例子可以很容易地推出：此时的费马方程也无非平凡解。限于篇幅，我们不再详细介绍。有兴趣的读者可以参看辛格所著的《费马大定理》或其他相关的科普书籍。

二、退化的椭圆曲线

上面我们定义的椭圆曲线方程 $y^2 = x^3+ax+b$ 要求系数满足 $4a^3+27b^2 \neq 0$.

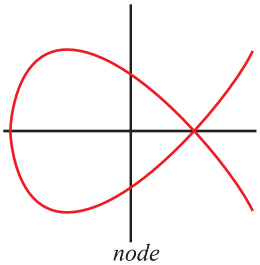
那么假如 $4a^3+27b^2 = 0$, 我们会得到什么样的三次方程的曲线呢？

$y^2 = x^3$



cusp

$y^2 = x^3 - 3x + 2$



node

(1) 带结点的有理曲线（a, b 不全为零）此时图形如上图图右。

大家可以看到，曲线上有一个自交点。 在这个交点附近看曲线类似于一个十字架，因此我们称之为结点 (node)。这里“有理曲线”一词可以粗略理解为指直线或圆锥曲线的意思。上述曲线图形可以差不多看成是这条有理曲线打了一个结——后面我们会解释这一点。

(2) 带尖点的有理曲线 ($a=b=0$) 此时图形示意图如上图左。

这条曲线有一个尖锐的点，称作尖点 (cusp)。顾名思义，这条曲线就好比是有理曲线上捏出一个尖点。

除了以上两种曲线，我们还把以下几类曲线都统称为退化的椭圆曲线：

(3) 三条直线的并集（即三条一次曲线的并集），

(4) 一条圆锥曲线和一条直线的并集（即一条二次曲线和一条一次曲线的并集）。

从这个泛化概念上看，我们可以把直线和圆锥曲线也看作是椭圆曲线的一个部分。因此，可以预见，圆锥曲线的很多美妙性质应该都来自于椭圆曲线。事实正是如此。

三、名不副实：为什么叫“椭圆曲线”?

椭圆曲线的图形和椭圆显然没什么关系（见前面的图）那为什么我们要称之为“椭圆曲线”呢？

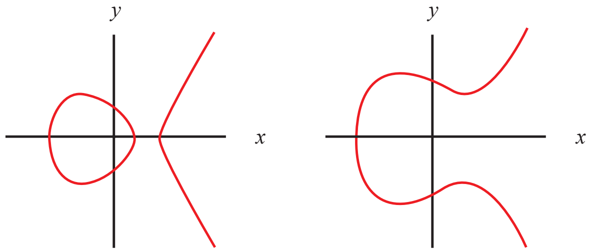
原来，当初人们想用微积分计算椭圆的周长（圆的周长大家都会求）。通过一定的积分技巧，最终要求出以下类型的积分：

$$\int_{a}^{\beta}\frac{dx}{\sqrt{x^3+ax+b}}$$

其中分母的函数项 $y=\sqrt{x^3+ax+b}$ 两边平方一下恰好就是椭圆曲线的方程。这就是为什么椭圆曲线的名字里包含“椭圆”二字。顺便说一下，上述积分是无法用初等函数的表达式计算出来的；而其本质原因和椭圆曲线的几何性质密切相关。

四、海底冰山：椭圆曲线隐藏的部分

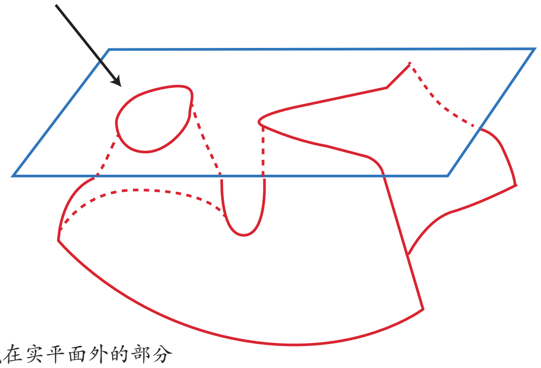
回顾一下，椭圆曲线的两个例子



从第一张图，我们可以看到椭圆曲线的图形似乎可以分离成两个不相交的分支，第二张图则只有一个分支。是否还有许多其他的类型呢？确实如此。牛顿曾经对椭圆曲线做了很细致的分类，将它们分成了数十种类型。

为什么直线和圆锥曲线只有区区几种类型，而椭圆曲线种类一下子增加很多呢？让我们先想象一个情景：在宽阔的海平面上露出一处礁石。如果海平面降低的话，礁石就会变大，可能会形成一座小山；如果海平面继续下降，本来的一座小山可能会变成许多座互不相连的小山；随着海平面下降，小山们变成了一座座小岛，有些本来不相连的岛甚至可能会连接起来。假如我们抽干所有的水，那么你会发现所有的岛其实只不过是同一块陆地的不同部分。

其实我们要解释的问题和上述比喻完全一样。 因为通常考虑的曲线上的点 (x, y) 都是实数点，即 x, y 是实数。假如我们允许 x, y 取复数，那么椭圆曲线上就多出了许许多多复数点。想象一下，实数坐标平面好比我们的海平面，包括全部复数点和实数点的椭圆曲线好比是陆地，其中露在海平面上的部分只是实数点（见以下示意图）。



这样一来，你看到的椭圆曲线实图形其实只是整个椭圆曲线中的很少一部分，大部分都隐藏在实坐标平面背后。海面上的岛屿千差万别，但实际上无非是同一块陆地的不同部分。这就是我们所要的答案——有点类似于“盲人摸象”的典故。

上面的讨论告诉我们，如果仅考虑实数情形的话，我们其实损失掉了很多有用的几何信息。仅考虑实数平面图形显然是一个不必要的思维枷锁。因此我们完全可以放弃掉这一假设，即允许 x, y 取复数。这样一来我们得到的椭圆曲线要比原来的丰富了许多！当然，为了以后画图方便，人们仍然习惯于用实数平面的图形作为椭圆曲线的示意图——上一节的几张图都是这样。以后我们谈到椭圆曲线就默认它是在复数坐标上的。